The University of North Texas at Dallas Policy Manual	Chapter 14.000
14.006 Password Protection	**Information Technology**

Policy Statement. It is the policy of the University of North Texas at Dallas to manage the University's information resources as strategic assets of the State of Texas. User authentication is a means to control who has access to an information resource system. Controlling the access is necessary for any information resource. The confidentiality, integrity, and availability of information can be lost when access is gained by a non-authorized entity. This policy defines the process for the creation, distribution, safeguarding, termination, and reclamation of the University user authentication mechanisms.

Application of Policy. This policy applies to all University Users.

Definitions.

1. Information Resources. "Information Resources" mean the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data and administered both centrally and within individual departments, on-campus and remotely, on a mainframe and network servers, and for use by single and multiple users.

2. Confidential Information. "Confidential Information" means information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements). Examples of confidential information include, but are not limited to: personally identifiable information, student education records, intellectual property, and medical records.

3. Mission Critical Information. "Mission Critical Information" means information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

4. Password. "Password" means a string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

5. Strong Password. "Stong Password" mean a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system.

6. Information Resource Owner. "Information Resource Owner" means an entity responsible for a business function and determining controls and access to information resources supporting that business function.

7. University Users. "University Users" mean all faculty, staff, students, contractors, volunteers, and individuals that maintain a business relationship with University that make use of University information resources requiring authentication. Information resources may also be included in this category.

Procedures and Responsibilities.

Password Administration. The information resource owner or designee is responsible for ensuring that measures are implemented to mitigate information security risks associated with password authentication. All passwords should, where applicable, be constructed and implemented according to the following criteria:

1. Servers that are mission critical and/or maintain confidential information shall require passwords.

2. Passwords must be treated as confidential information.

3. Creation.
   i. Passwords should not include content that can be easily associated with the account owner such as: user name, social security number, employee identification number, nickname, relative's name, birth date, telephone number, street name, favorite sport, etc.

   ii. Passwords should not be dictionary words regardless of language of origin.

4. Routine Changes.
   i. Passwords shall be routinely changed and change intervals will be established as appropriate for systems processing/storing mission critical and/or confidential data (e.g. 90 day intervals).

   ii. Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups, stored procedures) are not subject to the routine change

specified. System administrators shall document a separate risk management process for each such password.

iii. Where feasible, owners of systems that maintain mission critical and/or confidential information shall establish a reasonable period of time for passwords to be maintained in history to prevent their reuse.

5. Security.
   i. Stored passwords shall be encrypted.

   ii. Passwords shall never be transmitted as plain text.

   iii. There shall be a maximum number of tries established before a user is locked out of an account. Delay, or progressive delay, helps to prevent automated "trial-and-error" attacks on passwords.

   iv. Security tokens (e.g., Smartcard) must be returned when there has been a change in job duties which no longer require restricted access, or upon separation from the University.

   v. If the security of a password is in doubt, the password shall be changed immediately. If the password has been compromised, the event shall also be reported to the appropriate system administrator(s).

   vi. Forgotten passwords shall be replaced, not reissued.

   vii. Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or logging off device.

   viii. Users shall not circumvent password entry with auto logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store mission critical and/or confidential data. Users should always enter "no" when asked to have password "remembered."

6. Audit Trail.
   i. Where possible, passwords that are user selected shall be checked by a password audit system that adheres to the established criteria of the system or service.

   ii. Systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system.

iii. Where possible, password management and automated password generation must have the capability to maintain auditable transaction logs containing information such as: time and date of password change, expiration, administrative reset, type of action performed, and source system that originated the change request.

Responsible Party: Information Resource Owner/Information Technology/All University Users

References and Cross-references.

Texas Government Code § 2054 – Information Resources

Texas Administrative Code, Chapter 202, Subchapter C and Department of Information Resources, Policy and Standards for Protecting Information Resources for Texas

Texas Business & Commerce Code § 48.002

Family Educational Rights and Privacy Act

Texas Education Code § 51.914

Health Insurance Portability and Accountability Act of 1996

Approved: 8/30/2010
Effective: 8/30/2010
Revised: